ZeroLock®

Defense-in-Depth for Hypervisors

vs. Traditional Hypervisor Security Approaches

As enterprises grow their private cloud, threat actors have locked in on the hypervisor. Recognized by Gartner as a Key Startup in Security Software, Vali Cyber® has expanded our ZeroLock® platform to take a proactive, multilayer approach to hypervisor defense—answering this critical security gap.

Traditional Hypervisor Security

Hardening + Segmentation + EDR + Logs

Core Characteristics

- Hardening procedures are more manual and cumbersome, but can reduce vulnerability risk
- Segmentation can serve as a preventative control to reduce blast radius, but can miss key attack tactics like lateral movement
- Detection is implied, but records actions after they happen which doesn't help with fast moving attacks
- Cannot stop attacks once access is gained
- Relies on multiple tools that are likely agent-based and network-based

The overall security posture is reactive. In the event an environment is breached, the user must rely on back-ups (that may have the attacker still inside) or start anew.

ZeroLock

Defense-in-Depth for Hypervisors

Core Differentiators

- Preventative layers, including hardening procedures, CLI-MFA, anti-tampering, and virtual patching are automated to quickly and effectively enforce zero-trust exploit prevention
- Complements segmentation by being able to detect tactics like lateral movement at runtime for fast response
- Emphasis is on multiple prevention points, but detection and remediation exist as a last resort and happen in real-time automatically
- Stops ransomware, living-off-the land attacks, zero-days, and tampering
- Single tool that runs in user space, does not alter the hypervisor kernel, does not require connectivity for effectiveness, and plugs into existing SIEMs/SOARs for simplified management

The overall security posture is preventative and proactive. In the event an environment is breached, the attack can be stopped, and the system restored in seconds, helping to ensure business continuity.

Traditional hypervisor security is reactive—focused on hardening, segmentation, and logs after compromise. ZeroLock's Defense-in-Depth for Hypervisors stops attacks before they start, giving your team peace of mind and ensured business continuity.

Schedule your demo today! info@valicyber.com

valicyber®

Vali Cyber® and ZeroLock® are trademarks of Vali Cyber, Inc.
All other trademarks are the property of their respective owners.

©Vali Cyber, Inc. | valicyber.com

ZeroLock

ZeroLock Endpoint Agent Requirements for Hypervisors

OS	• VMware Cloud Foundation 9.X • VMware ESX, 6.7+ (Older versions supported on request.) • Nutanix-managed ESX, 6.7+ • Nutanix AHV 2017+* • XenServer, 6.5+ • Citrix Hypervisor, 8.0+ • XCP-ng 8.3+ • Proxmox, 3.0+ • Red Hat Enterprise Virtualization, 3.6+ • HPE Morpheus, 8.0+ • Dell VxRail, 4.8+ • KVM, Kernel 3.5+ *Nutanix does not currently support third-party products running on AHV.
Processor	x86-64, ARM-64 (coming soon)
Memory	50MB
Disk Space	100MB
Kernel Mods	No kernel modification or modules required
Installation Methods	• One-line, web-based deployment (Wget) • File-based deployment (Tar.gz or Bash) • VCF & ESXi: Signed VIB and deployable via vCenter

ZeroLock Server Requirements (Only required for on-prem deployment.)

RAM	16GB
Disk Space	128GB (Dependent on number of endpoints and data retention period.)
CPU Cores	6 or more recommended
Installation Reqs.	• Self-deployment: Latest version of Docker installed • OVA-deployment: ESXi 7.0 or later

ZeroLock Bidirectional API-First Architecture

Documentation	Visit api.zerolock.com for a full API
Existing Integrations	• SIEM: Splunk, Sumo Logic, Elastic, Google SecOps, CrowdStrike Next-Gen • SOAR: Swimlane • Incident API: Veeam

About Vali Cyber

Vali Cyber® secures the core of enterprise infrastructure: the hypervisor and the management plane that controls it. Most defenses stop at the endpoint, but attackers have moved below it, where one compromise can take down every workload. A pioneer of preemptive hypervisor security, Vali Cyber built ZeroLock® for defense-in-depth: CLI-MFA and exploit prevention stop attacks before they start, AI behavioral detection catches what can get past, and automated rollback restores workloads in seconds. One lightweight agent protects most major hypervisors and streams every event into the SIEM and SOAR tools teams already use. Recognized by Gartner as a Key Startup in Security Software, Vali Cyber protects the layer others overlook.



MADE IN THE U.S.A.

valicyber®

Vali Cyber® and ZeroLock® are trademarks of Vali Cyber, Inc.
All other trademarks are the property of their respective owners.

©Vali Cyber, Inc. | valicyber.com